Journal of Algebra 322 (2009) 2286–2296

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On non-solvable Camina pairs

Zvi Arad [a], Avinoam Mann [b], Mikhail Muzychuk [a,*], Cristian Pech [c]

[a] Department of Computer Sciences and Mathematics, Netanya Academic College, University St. 1, 42365, Netanya, Israel
[b] Einstein Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
[c] Department of Mathematics, Ben-Gurion University, Beer-Sheva, Israel

ARTICLE INFO

Article history:
Received 27 September 2008
Available online 29 July 2009
Communicated by Martin Liebeck

Keywords:
Camina pair

ABSTRACT

In this paper we study non-solvable and non-Frobenius Camina pairs (G, N). It is known [D. Chillag, A. Mann, C. Scoppola, Generalized Frobenius groups II, Israel J. Math. 62 (1988) 269–282] that in this case N is a p-group. Our first result (Theorem 1.3) shows that the solvable residual of $G/\mathbf{O}_p(G)$ is isomorphic either to $SL(2, p^e)$, p is a prime or to $SL(2, 5)$, $SL(2, 13)$ with $p = 3$, or to $SL(2, 5)$ with $p \geqslant 7$.

Our second result provides an example of a non-solvable and non-Frobenius Camina pair (G, N) with $|\mathbf{O}_p(G)| = 5^5$ and $G/\mathbf{O}_p(G) \cong SL(2, 5)$. Note that G has a character which is zero everywhere except on two conjugacy classes. Groups of this type were studies by S.M. Gagola [S.M. Gagola, Characters vanishing on all but two conjugacy classes, Pacific J. Math. 109 (1983) 363–385]. To our knowledge this group is the first example of a Gagola group which is non-solvable and non-Frobenius.

1. Introduction

Let G be a finite group. A pair (G, N), $N \trianglelefteq G$ is called a *Camina pair* [3] if

$$\forall g \in G \setminus N, \quad gN \subset g^G, \tag{1}$$

i.e. each element $g \notin N$ is conjugate to all the elements in the coset gN. The subgroup N will be referred to as the *Camina kernel*.

* Corresponding author.
E-mail addresses: aradtzvi@netanya.ac.il (Z. Arad), mann@math.huji.ac.il (A. Mann), mikhail@netvision.net.il (M. Muzychuk).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.06.023

In [3] A.R. Camina proved that if (G, N) is a Camina pair then it is Frobenius group or at least one of the groups G/N, N is a p-group.

D. Chillag, A. Mann and C. Scoppola proved in [6] that G is solvable if G/N is a p-group. So for a non-solvable Camina pair (G, N) the subgroup N is a p-group or G is Frobenius. All non-solvable Frobenius groups are well known (see [11]). In this paper we focus on non-solvable and non-Frobenius Camina pairs.

Given a Camina pair as above, with N a p-group, let $g \in G$ be a p'-element, of order q, say. If g commutes with an element $1 \neq n \in N$, where n has order p^e, then gn has order $qp^e \neq q$, and thus g and gn are not conjugate. Therefore g commutes with no non-identity element in N.

$G/\Phi(N)$ is also a Camina group, with an elementary abelian kernel $V = N/\Phi(N)$.

In [4] P. Fleischmann, W. Lempken and P.H. Tiep say that a group G is *p'-semiregular* on a finite-dimensional $\mathbb{F}[G]$ module V defined over some field $\mathbb{F}$, if every p'-element of G acts without fixed points on the set $V \setminus \{0\}$.

Let $\mathcal{R}$ be the set of primes r satisfying the following conditions

(a) $r = 2^a \cdot 3^b + 1$ for $a \geqslant 2$, $b \geqslant 0$;
(b) $(r+1)/2$ is a prime, or $r = 7$ or 17.

Theorem 4.2 of [4] states the following

Theorem 1.1. *Let G be a non-trivial perfect finite group with $\mathbf{O}_p(G) = 1$ and $p \mid |G|$, and let G act p'-semiregularly on a G-module V of characteristic p. Then one of the following holds*

(a) $G \cong SL(2, p^a)$ *for some* $a \geqslant 1$ *and* $p^a > 3$;
(b) $G \cong Sz(2^{2a+1})$ *for some* $a \geqslant 1$ *and* $p = 2$;
(c) $G \cong Sz(2^{2a+1}) \times SL(2, 2^{2b+1})$ *for some* $a, b \geqslant 1$ *and* $\gcd(2a+1, 2b+1) = 1$, *and* $p = 2$;
(d) $G \cong SL(2, r)$ *with* $r \in \mathcal{R}$ *and* $p = 3$.

Conversely, if (G, p) satisfies any of the conditions (a)–(d)*, then there exists a faithful absolutely irreducible G-module V in characteristic p such that G acts p'-semiregularly on V.*

In view of our earlier remarks, this has the following

Corollary 1.2. *Let (G, N) be a Camina pair such that G is not solvable. If N is a p-group and p divides the order of $(G/\mathbf{O}_p(G))^\infty$, then one of the following holds*

(a) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, 2^n)$, $Sz(2^{2m+1})$ *and* $p = 2$;
(b) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, 2^{2a+1}) \times Sz(2^{2b+1})$ *with* $\gcd(2a+1, 2b+1) = 1$ *and* $p = 2$;
(c) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, 3^n)$ *or* $(G/\mathbf{O}_p(G))^\infty \cong SL(2, r)$, $r \in \mathcal{R}$ *and* $p = 3$;
(d) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, p^n)$ *and* $p \geqslant 5$.

Here X^∞ denotes the solvable residual of the group X, i.e. the last term in the derived series $X^{(d)}$.

Our first result eliminates most of the cases. More precisely, we prove the following

Theorem 1.3. *Let (G, N) be a Camina pair such that G is non-solvable. Then N is a p-group and one of the following holds*

(a) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, p^e)$, $p^e > 3$;
(b) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, 5)$, $p = 3$;
(c) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, 13)$, $p = 3$;
(d) $(G/\mathbf{O}_p(G))^\infty \cong SL(2, 5)$, $p \geqslant 7$ *and* $(\mathbf{S}(G), N)$ *is a Camina pair*; $G/\mathbf{S}(G) \cong A_5$ *or* S_5 (*here* $\mathbf{S}(G)$ *denotes the solvable radical of* G).

If N is minimal, then by Proposition 2.2 the factor-group $G/\mathbf{O}_p(G)$ acts faithfully on N by conjugation. So, N affords a natural structure of a faithful irreducible $\mathbb{F}_p[G/\mathbf{O}_p(G)]$-module on which $G/\mathbf{O}_p(G)$ acts p'-semiregularly. Considering N as an $\mathbb{F}_p[(G/\mathbf{O}_p(G))^\infty]$-module we conclude, by Clifford's theorem, that N is isomorphic to direct sum of simple $\mathbb{F}_p[(G/\mathbf{O}_p(G))^\infty]$-modules, say $N_1 \oplus \cdots \oplus N_k$. On each of these modules the group $(G/\mathbf{O}_p(G))^\infty$ acts p'-semiregularly. All simple $\mathbb{F}_p[SL(2,\ell)]$-modules with p'-semiregular action of $SL(2,\ell)$ were classified in [4]. This yields the following

Corollary 1.4. *Each of the N_i's is isomorphic to*

(a) *the natural 2-dimensional module of $SL(2,p^e)$ if $(G/\mathbf{O}_p(G))^\infty \cong SL(2,p^e)$, $p^e > 3$;*
(b) *one of the two 4-dimensional $\mathbb{F}_3[SL(2,5)]$-modules if $(G/\mathbf{O}_p(G))^\infty \cong SL(2,5)$, $p = 3$;*
(c) *one of the two 6-dimensional $\mathbb{F}_3[SL(2,13)]$-modules if $(G/\mathbf{O}_p(G))^\infty \cong SL(2,13)$, $p = 3$;*
(d) *a 2 or 4-dimensional $\mathbb{F}_p[SL(2,5)]$-module if $(G/\mathbf{O}_p(G))^\infty \cong SL(2,5)$, $p \geqslant 7$.*

Notice that in the latter case the dimension of an $\mathbb{F}_p[SL(2,5)]$-module is two if and only if 5 and -1 are squares in $\mathbb{F}_p$.

Our second result provides an example of a non-solvable and non-Frobenius Camina pair (G,N) with $|G| = 2^3 \cdot 3 \cdot 5^6$ (see Section 3). The group G has a character which is zero everywhere except on two conjugacy classes. Groups of this type were studied by S.M. Gagola [5]. To our knowledge, this group is the first example of a Gagola group which is non-solvable and non-Frobenius.

Arad and Blau [1] and Mann [10] studied finite groups G which have two distinct irreducible characters χ and η satisfying

$$\chi\eta = m\chi + n\eta \quad \text{with } m,n > 0. \tag{2}$$

The interest in this situation arises because of the fact that very little is known about the decomposition into irreducibles of the product of two irreducible characters, thus there is interest even in such extreme assumptions as (2).

It was shown in [2] that G is not simple. Following that, Arad and Blau [1] and Mann [10] proved the following

Theorem 1.5. *Let G be a finite group satisfying* (2)*. Then χ and η have the same kernel, say M, and there exists a normal subgroup N of G such that*

(a) *$M \subset N$ and N/M is an elementary abelian minimal normal subgroup of G/M;*
(b) *$(G/M, N/M)$ is a Camina pair with Camina kernel N/M;*
(c) *N/M consists of the identity and two non-trivial conjugacy classes, which are real.*

Conversely, a Camina pair with an elementary abelian kernel N consisting of the identity and two non-identity real classes has two faithful irreducible characters satisfying (2)*.*

As a corollary of Theorem 1.3 we obtain the following

Theorem 1.6. *Let G be as in Theorem* 1.5*. Assume that G is non-solvable and non-Frobenius. Then $|N/M| = 3^4$, $N \subset \mathbf{O}_3(G)$ and $(G/\mathbf{O}_3(G))^\infty \cong SL(2,5)$.*

We have no example of such groups.

The paper is organized as follows. The next section contains the proof of Theorems 1.3 and 1.6. Section 3 describes the example mentioned above.

All the notations used in the paper are standard.

2. Proof of Theorems 1.3 and 1.6

We start with the following statement

Proposition 2.1. *Let (G, N) be a Camina pair and $\chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N)$ an arbitrary character. Denote by ℓ_χ the number of irreducible characters of N appearing in χ_N, and by e_χ their multiplicity in χ_N. Then $e_\chi^2 \ell_\chi = [G : N]$. In particular, the ratio ℓ_χ/ℓ_η, $\chi, \eta \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N)$ is a square of a rational number.*

Proof. Write $\chi_N = e(\theta_1 + \cdots + \theta_\ell)$ where $\theta_i \in \mathrm{Irr}(N)$. Recall that χ vanishes outside N [3]. Thus

$$1 = |G|^{-1} \sum_{g \in G} \chi(g)\overline{\chi(g)} = |G|^{-1} \sum_{g \in N} \chi(g)\overline{\chi(g)} = |G|^{-1} \sum_{g \in N} e^2 \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} \theta_i(g)\overline{\theta_j(g)}$$

$$= [G : N]^{-1} e^2 \sum_{i=1}^{\ell} \sum_{j=1}^{\ell} (\theta_i, \theta_j)_N = [G : N]^{-1} e^2 \ell. \qquad \square$$

Let G be a finite group and p a prime dividing $|G|$. We say that G has the NS_p*-property* if any irreducible p'-semiregular $\mathbb{F}_p[G]$-module V contains two non-zero vectors v, w such that $|Gv|/|Gw|$ is not a square (where Gv denotes the G-orbit of the vector v). Since the stabilizer of a non-zero vector in V is a p-group, the ratio $|Gv|/|Gw|$ is always a p-power. Notice that since $|V|$ is a p-power, a Sylow p-subgroup of G fixes at least $p - 1$ non-zero vectors of V. In particular, there always exists a G-orbit of p'-cardinality.

Proposition 2.2. *Let (G, N) be a Camina pair with N being a minimal normal p-subgroup. Then $\mathbf{C}_G(N) = \mathbf{O}_p(G)$ and $G/\mathbf{O}_p(G)$ does not have the NS_p-property.*

Proof. First, let us show that $\mathbf{C}_G(N) = \mathbf{O}_p(G)$. Since $\mathbf{C}_G(n)$, $n \in N^\#$ is a p-group, we obtain that $\mathbf{C}_G(N) \trianglelefteqslant \mathbf{O}_p(G)$. Since (G, N) is a Camina pair and N is minimal, N is the unique minimal subgroup of G. Hence $N \leqslant \mathbf{Z}(\mathbf{O}_p(G))$ implying $\mathbf{C}_G(N) = \mathbf{O}_p(G)$. Thus the group $\overline{G} := G/\mathbf{O}_p(G)$ acts faithfully on N. Since N is minimal, it is elementary abelian and affords a natural structure of $\mathbb{F}_p[G]$-module. Each p'-element of G acts on $N - \{1\}$ semiregularly. Therefore N is an irreducible p'-semiregular $\mathbb{F}_p[G]$-module. The dual module N^* is also an irreducible p'-semiregular $\mathbb{F}_p[G]$-module. The action of $\overline{G}$ on the vectors of N^* is equivalent to the action of $\overline{G}$ on $\mathrm{Irr}(N)$. Therefore the orbit lengths of the two actions coincide. Each orbit of $\overline{G}$ on $\mathrm{Irr}(N)$ consists of the characters that appear in a decomposition of χ_N for certain $\chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(G/N)$. It follows from Proposition 2.1 that the ratio between the sizes of two non-trivial $\overline{G}$-orbits on $\mathrm{Irr}(N)$ is always a square. Hence the same property holds for non-trivial orbits of $\overline{G}$ on N^*. $\square$

Proposition 2.3. *Let X be a central product of its subgroups G and F. If G has the NS_p-property, then so does X.*

Proof. Let V be a p'-semiregular irreducible $\mathbb{F}_p[X]$-module and U a minimal (non-trivial) $\mathbb{F}_p[G]$ submodule of V. Then U is an irreducible p'-semiregular $\mathbb{F}_p[G]$-module. Since G has the NS_p property, there exist non-zero $u_1, u_2 \in U$ for which the ratio $|Gu_1|/|Gu_2|$ is a non-square. Thus $|Gu_1|/|Gu_2| = p^\alpha$ where α is an odd integer. We are going to show that $|Xu_1|_p/|Xu_2|_p = p^\alpha$, thereby proving the statement.

Since F centralizes G, the sets fGu_i, $f \in F$ are G-orbits as well. Let F_i be the setwise stabilizer in F of the orbit Gu_i. Then $|Xu_i| = |FGu_i| = [F : F_i]|Gu_i|$. Since Gu_i is F_i-invariant, the module U is F_i-invariant too. In other words, F_i is a subgroup of $F_{\{U\}} := \{f \in F \mid fU = U\}$. Let F_U be the kernel of the action of $F_{\{U\}}$ on U. Then $F_{\{U\}}/F_U$ is embedded into $\mathrm{End}_{\mathbb{F}_p[G]}(U)$. Since U is $\mathbb{F}_p[G]$-irreducible, $\mathrm{End}_{\mathbb{F}_p[G]}(U)$ is a division algebra by Schur's lemma. But $\mathrm{End}_{\mathbb{F}_p[G]}(U)$ is finite. Therefore,

by Wedderburn's theorem, $\mathsf{End}_{\mathbb{F}_p[G]}(U)$ is a field. Thus $F_{\{U\}}/F_U$ is embedded into the multiplicative group of a finite field of characteristic p, implying $|F_{\{U\}}/F_U|_p = 1$. Together with $F_U \leqslant F_i \leqslant F_{\{U\}}$ we obtain $|F_i/F_U|_p = 1$. Therefore

$$[F : F_i]_p = \frac{|F|_p}{|F_i|_p} = \frac{|F|_p}{|F_U|_p} \cdot \frac{|F_U|_p}{|F_i|_p} = \frac{|F|_p}{|F_U|_p} \quad \Rightarrow \quad [F : F_1]_p = [F : F_2]_p.$$

Now the following line finishes the proof

$$\frac{|Xu_1|_p}{|Xu_2|_p} = \frac{[F : F_1]_p |Gu_1|_p}{[F : F_2]_p |Gu_2|_p} = \frac{|Gu_1|_p}{|Gu_2|_p} = p^\alpha. \qquad \square$$

We are ready now to prove Theorem 1.3. As before let (G, N) be a Camina pair with non-solvable G. If M is a normal subgroup of G contained in N, then $(G/M, N/M)$ is also a Camina pair. So, without loss of generality we may assume that N is a minimal normal p-subgroup of G. We also may assume that G/G' is a p-group. Indeed, if G/G' is not a p-group, then G contains a normal subgroup M of prime index distinct from p. In this case Theorem 5.4 of [8] implies that (M, N) is a Camina pair. So we can replace G by M in this case.

Since $\mathbf{C}_G(N) = \mathbf{O}_p(G)$, the factor-group $\overline{G} := G/\mathbf{O}_p(G)$ acts faithfully on N. This action is p'-semiregular, because (G, N) is a Camina pair. The group $\overline{G}^\infty$ is perfect and acts on N p'-semiregularly. We split our proof into two cases depending on whether p divides $|\overline{G}^\infty|$ or not.

Case A. $p \nmid |\overline{G}^\infty|$.

In this case $\overline{G}^\infty$ acts fixed-point-freely on $N \setminus \{1\}$. Therefore $N \rtimes \overline{G}^\infty$ is a Frobenius group with perfect complement. Now Zassenhaus' theorem implies that $\overline{G}^\infty \cong SL(2, 5)$. In particular, $p \geqslant 7$.

Let $L \leqslant G$ be an overgroup of $\mathbf{O}_p(G)$ such that $L/\mathbf{O}_p(G) \cong \mathbf{C}_{\overline{G}}(\overline{G}^\infty)$. Since $\mathbf{C}_{\overline{G}}(\overline{G}^\infty)$ is solvable, L is a normal solvable subgroup of G. It follows from $G/L \cong \overline{G}/\mathbf{C}_{\overline{G}}(\overline{G}^\infty)$ that G/L is embedded into $\mathsf{Aut}(\overline{G}^\infty) \cong \mathsf{Aut}(SL(2, 5)) \cong S_5$. Together with $\mathsf{Inn}(\overline{G}^\infty) \leqslant \overline{G}/\mathbf{C}_{\overline{G}}(\overline{G}^\infty)$ we obtain that G/L is isomorphic either to A_5 or S_5. In particular, $L = \mathbf{S}(G)$. Since L is a normal subgroup of G of p'-index, Theorem 5.4 [8] implies that (L, N) is a Camina pair.

Case B. $p \mid |\overline{G}^\infty|$.

By Theorem 1.1, $\overline{G}^\infty$ is one of the following groups

(a) $\overline{G}^\infty \cong SL(2, p^a)$ for some $a \geqslant 1$ and $p^a > 3$;
(b) $\overline{G}^\infty \cong Sz(2^{2a+1})$ for some $a \geqslant 1$ and $p = 2$;
(c) $\overline{G}^\infty \cong Sz(2^{2a+1}) \times SL(2, 2^{2b+1})$ for some $a, b \geqslant 1$ and $\gcd(2a + 1, 2b + 1) = 1$, and $p = 2$;
(d) $\overline{G}^\infty \cong SL(2, r)$ with $r \in \mathcal{R}$ and $p = 3$.

By Proposition 2.2 the group $\overline{G}$ does not have the NS_p-property. Thus in order to exclude the cases (b)–(d) it suffices to show that the groups mentioned there have the NS_p-property.

The group $\overline{G}/(\overline{G}^\infty \mathbf{C}_{\overline{G}}(\overline{G}^\infty))$ is embedded into $\mathsf{Out}(\overline{G}^\infty)$. In the cases (b)–(d), $\mathsf{Out}(\overline{G}^\infty)$ is an abelian group of p'-order. Since G/G' is a p-group, $\overline{G}/\overline{G}'$ is a p-group as well. Therefore $\overline{G} = \overline{G}^\infty \mathbf{C}_{\overline{G}}(\overline{G}^\infty)$ in the last three cases. By Proposition 2.3 it suffices to show that $\overline{G}^\infty$ has the NS_p-property.

Case (b). The group $Sz(2^{2a+1})$ has the NS_2-property.

By Proposition 4.9 of [4] the only $2'$-semiregular module for $Sz(q), q = 2^{2a+1}$ is the natural one of dimension 4 over $\mathbb{F}_q$. The group $Sz(q)$ has two orbits in its action on non-zero vectors, of cardinalities $(q^2 + 1)(q - 1)$ and $q(q^2 + 1)(q - 1)$ (see, for example, [9]). Their ratio is $q = 2^{2a+1}$ a non-square.

Case (c). The group $Sz(2^{2a+1}) \times SL(2, 2^{2b+1})$ has the NS_2-property.

This follows from the case (b) and Proposition 2.3.

Case (d). The group $SL(2, r)$ with $r \in \mathcal{R}$ has the NS_3-property for $r \neq 5, 13$.

Let V be a $3'$-semiregular $\mathbb{F}_3[SL(2, r)]$-module of dimension d and let ρ denote the corresponding representation.

Assume first that a Sylow 3-subgroup of $SL(2, r)$ is of order 3. First note that if $3 \nmid (r-1)$, then either $r = 17$ or $r = 2^a + 1$. The first case contradicts $|SL(2, r)|_3 = 3$. In the second case the conditions (a)–(b) which define $\mathcal{R}$ imply $r = 5$. So, we may assume that $3 \mid (r-1)$. Note that in this case $r = 2^a \cdot 3 + 1$.

The stabilizer of a non-zero vector $v \in V$ is a 3-subgroup of $SL(2, r)$. Hence its order is either 3 or 1. If there are two non-zero vectors with stabilizers of distinct orders, then the corresponding orbit ratio is 3 and we are done. Assume the contrary. Then a stabilizer of each non-zero vector has order 3. Therefore all $SL(2, r)$-orbits on $V \setminus \{0\}$ have the same length, and their number is $3(3^d - 1)/|SL(2, r)|$. Since $3 \mid (r-1)$, the group $SL(2, r)$ has $r^2 + r$ elements of order 3 which are pairwise conjugate. Let g be one of them. Denote by s the dimension of a fixed-point subspace $\mathsf{Fix}(g)$ of g. Then each element of order 3 fixes $3^s - 1$ elements and, by Cauchy–Frobenius lemma, we obtain $(3^d - 1)2 = (r^2 + r)(3^s - 1)$, or, equivalently, $3^d - 1 = \frac{r^2+r}{2}(3^s - 1)$. So, $(3^s - 1) \mid (3^d - 1)$ implying $s \mid d$. Since $\rho(g) \in GL_d(\mathbb{F}_3)$ is a matrix of order 3, $s = \dim(\mathsf{Fix}(g)) \geqslant d/3$. Therefore either $d = 2s$ or $d = 3s$. In the first case we obtain $3^s + 1 = \frac{r^2+r}{2}$, in the second one $3^{2s} + 3^s + 1 = \frac{r^2+r}{2}$.

It follows from $r - 1 = 2^a \cdot 3$ that a centralizer of g in $SL(2, r)$ contains a subgroup of order 2^a. This subgroup leaves $\mathsf{Fix}(g)$ invariant and acts on it fixed-point-freely. Therefore 2^a divides $3^s - 1$.

If $3^s + 1 = \frac{r^2+r}{2}$, then $3^s + 1 = (2^a \cdot 3 + 1)(2^{a-1} \cdot 3 + 1)$. Comparing both sides modulo 2^a yields us $2 \equiv 2^{a-1} + 1 \pmod{2^a}$ which is possible only if $a = 1$. In this case we get $r = 7$, $s = 3$, $d = 6$. Hence the number of orbits of $SL(2, 7)$ is $3(3^6 - 1)/(6 \cdot 7 \cdot 8) = 13/2$, a contradiction.

If $3^{2s} + 3^s + 1 = \frac{r^2+r}{2}$, then $3^{2s} + 3^s + 1 = (2^a \cdot 3 + 1)(2^{a-1} \cdot 3 + 1)$. Comparing both sides modulo 2^a yields us $3 \equiv 2^{a-1} + 1 \pmod{2^a}$ which implies $a \leqslant 2$. Since $a = 1$ is impossible, $a = 2$ implying $r = 13$, $s = 2$, $d = 6$. In this case the number of orbits of $SL(2, 13)$ is one, that is $SL(2, 13)$ acts transitively on $V \setminus \{0\}$.

Assume now that $3^e := |SL(2, r)|_3 > 3$. Let P be a Sylow 3-subgroup of $SL(2, r)$. It is a cyclic group of order 3^e. Let g be a generator of P. Let n be the degree of the minimal polynomial of $\rho(g) - I_V$ (that is the minimal polynomial is x^n). Since $o(g) = 3^e$, we obtain $3^{e-1} < n \leqslant 3^e$. Let $v \in V$ be such that $(\rho(g) - I_V)^{n-1} v \neq 0$. Set $v_i := (\rho(g) - I_V)^{n-i} v$, $1 \leqslant i \leqslant n$. Then $(\rho(g) - I_V)^i v_i = 0$ and $v_1, \ldots, v_n = v$ are non-zero vectors. We claim that the stabilizers of v_1 and v_3 have orders 3^e and 3^{e-1} respectively (note that $v_3 \neq 0$, since $n > 3^{e-1} \geqslant 3$). Indeed $\rho(g)v_1 = v_1$ implying that $\langle g \rangle$ stabilizes v_1. But this is a Sylow 3-subgroup and the action is p'-semiregular. Therefore the stabilizer of v_1 has order 3^e. Consider now the stabilizer of v_3. By construction of v_3 its stabilizer contains $\langle g^3 \rangle$ of order 3^{e-1}. If the stabilizer is bigger then it should be a Sylow 3-subgroup of $SL(2, r)$. Since $g^3 \neq 1$, it is contained in a unique Sylow 3-subgroup, namely $\langle g \rangle$. But g does not fix v_3. Hence the stabilizer of v_3 has order 3^{e-1}. Finally $|Gv_3|/|Gv_1| = 3$, proving case (d).

We are now ready to prove Theorem 1.6. For this purpose we recall a definition of a Zsigmondy prime divisor. Let p be a prime and d a non-negative integer. A prime divisor z of $p^d - 1$ is called a Zsigmondy prime divisor of $p^d - 1$ if it does not divide $p^k - 1$ for all $1 \leqslant k < d$. By a theorem of Zsigmondy [13] such a prime always exists unless $(p, d) = (2, 6)$ or $d = 2$ and p is a Mersenne prime. Notice that we always have that $z > d$.

Proof of Theorem 1.6. We may assume that M is trivial. Then (G, N) is a Camina pair where N is minimal and normal, and, therefore it is elementary abelian, say of order p^d. As we have shown before, $\mathbf{O}_p(G) = \mathbf{C}_G(N)$. So, $\overline{G} := G/\mathbf{O}_p(G)$ acts faithfully on N which converts N to a faithful irre-

ducible $\mathbb{F}_p[\overline{G}]$-module. Since (G, N) is a Camina pair, this module is also p'-semiregular. Therefore the cardinality of each $\overline{G}$-orbit on $N - \{1\}$ is divisible by $k := |\overline{G}|_{p'}$.

Let C and D be the two non-trivial conjugacy classes of G contained in N. Both of them are orbits of $\overline{G}$. Since the action of $\overline{G}$ on N is p'-semiregular, the cardinality of these classes are k and kp^f for some non-negative integer f. Without loss of generality we may assume that $|C| = k$, $|D| = kp^f$. Since N is a minimal normal subgroup of G, we obtain $C^2 = D^2 = N$.

It follows from $C \cup D = N \setminus \{1\}$ that

$$p^d - 1 = k\left(p^f + 1\right) \tag{3}$$

implying $2f \mid d$ for non-zero f.

We need the following claim

Proposition 2.4. *If $p^d - 1$ has a Zsigmondy prime divisor z, say, then z divides $|\mathrm{Aut}(\overline{G}^\infty)|$.*

Proof. First we show that z divides k. Indeed, if not, then z divides $p^f + 1$ and, therefore $z \mid (p^{2f} - 1)$. Together with $2f \mid d$ this implies $d = 2f$, and, consequently, $k = p^f - 1$. It follows from $C^2 = N$ that $|D| \leqslant |C|^2$, contrary to $|D| = p^f(p^f - 1) > |C|^2$. Thus z divides k, and, therefore $z \mid |\overline{G}|$.

If z does not divide $|\mathrm{Aut}(\overline{G}^\infty)|$, then it divides $\mathbf{C}_{\overline{G}}(\overline{G}^\infty)$. Let Z be a cyclic subgroup of $\mathbf{C}_{\overline{G}}(\overline{G}^\infty)$ of prime order z. Since z is a Zsigmondy prime divisor of $p^d - 1$, the group Z acts on N irreducibly. Therefore the centralizer of Z in $\mathrm{Aut}(N) \cong GL(d, p)$ is a cyclic group. But this centralizer contains a non-solvable group $\overline{G}^\infty$, a contradiction. □

By Theorem 1.3 there are four possible cases for $\overline{G}^\infty$. We consider them one by one.

Case (A). $\overline{G}^\infty \cong SL(2, p^e)$, $p^e > 3$.

In this case $p^{2e} - 1$ divides k implying $d > 2e$. In particular $d \geqslant 3$. We claim that $p^d - 1$ has a Zsigmondy prime divisor. Indeed, if not then $d = 6$, $p = 2$ and either $k = 21$, $f = 1$ or $k = 7$, $f = 3$. The only possibility when $2^{2e} - 1$ divides one of the numbers $7, 21$ is $e = 1$ which contradicts the assumption $p^e > 3$. Thus $p^d - 1$ has a Zsigmondy prime divisor, say z. By Proposition 2.4 z divides $|\mathrm{Aut}(SL(2, p^e))| = p^e(p^{2e} - 1) \cdot e$. Since $2e < d$, z is coprime to $p^{2e} - 1$. Since $z > d > 2e$, z is coprime to e. Hence z is coprime to $|\mathrm{Aut}(\overline{G}^\infty)|$, contrary to Proposition 2.4.

Case (B). $\overline{G}^\infty \cong SL(2, 5)$, $p = 3$.

In this case we obtain $k(3^f + 1) = 3^d - 1$. It follows from $|\overline{G}^\infty|_{p'} \mid k$ that $40 \mid k$ and consequently $40 \mid (3^d - 1) \Rightarrow d = 4t$ for some non-negative integer t. If $d = 4$, then we are done. Assume that $d > 4$, that is $d \geqslant 8$. The number $3^d - 1$ has a Zsigmondy prime divisor z, say. It follows from $z > d \geqslant 8$ that $z \geqslant 11$. But in this case z is co-prime to $|\mathrm{Aut}(SL(2, 5))| = 120$, contrary to Proposition 2.4.

Case (C). $\overline{G}^\infty \cong SL(2, 13)$, $p = 3$.

It follows from $|\overline{G}^\infty|_{p'} \mid k$ that $8 \cdot 7 \cdot 13 \mid k$ and consequently $8 \cdot 7 \cdot 13 \mid (3^d - 1) \Rightarrow d = 6t$ for some non-negative integer t. If $d = 6$, then (3) implies $3^f + 1 = 1$ which is impossible. Therefore $d \geqslant 12$. The number $3^d - 1$ has a Zsigmondy prime divisor z, say. It follows from $z > d$ that z is at least 13. But 13 divides $3^6 - 1$. Therefore $z \geqslant 17$ implying that z is co-prime to $|\mathrm{Aut}(SL(2, 13))|$, contrary to Proposition 2.4.

Case (D). $\overline{G}^\infty \cong SL(2, 5)$, $p \geqslant 7$.

Note that in this case $|\overline{G}^{\infty}|$ is coprime to p, and, therefore, acts fixed-points-freely on $N \setminus \{1\}$.

Case (D1). $\overline{G}$ is a p'-group.

In this case $k = |\overline{G}|$, $f = 0$ implying $|\overline{G}| = (p^d - 1)/2$. We identify N with $\mathbb{Z}_p^d$ and consider $\overline{G}$ as a subgroup of $GL(d, p)$ of order $(p^d - 1)/2$ acting fixed-point-freely on the non-zero vectors.

First, we exclude the case of $d = 2$. Consider the image X of $\overline{G}$ in $PGL(2, p)$. It contains A_5, since A_5 is the image of $\overline{G}^{\infty} \cong SL(2, 5)$ in $PGL(2, p)$. According to [7] A_5 is maximal in $PSL(2, p)$. Since X is a p'-group, $X \cap PSL(2, p)$ is a proper subgroup of $PSL(2, p)$. Therefore, $|X \cap PSL(2, p)| = 60$ implying $|X| = 60$ or $|X| = 120$. Since A_5 is self-normalizing in $PGL(2, p)$, we obtain $|X| = 60$. Denoting $R := \overline{G} \cap \mathbf{Z}(GL(2, p))$ we obtain $|\overline{G}| = 60 \cdot |R|$. Together with $|\overline{G}| = (p^2 - 1)/2$ and $|R| \mid (p - 1)$ we obtain $(p + 1) \mid 120$. Now the condition $120 \mid \frac{p^2-1}{2}$ implies that no such prime exists.

Thus we may assume that $d \geqslant 3$. In this case $p^d - 1$ has a Zsigmondy prime divisor, say z. By Proposition 2.4 z is either 3 or 5. Since $z > d \geqslant 3$, the only option is $z = 5$ and $d = 3, 4$. Since $z = 5$, each cyclic subgroup of $\overline{G}$ of order 5 acts irreducibly on N. Therefore $\overline{G}^{\infty}$ also acts irreducibly on N. Therefore $\mathbf{C}_{GL(d,p)}(\overline{G}^{\infty})$ is a cyclic group the order of which divides either $p - 1$ or $p^2 - 1$ (in the latter case $d = 4$). Set $n := |\mathbf{C}_{\overline{G}}(\overline{G}^{\infty})|$. Since $\overline{G}/(\overline{G}^{\infty}\mathbf{C}_{\overline{G}}(\overline{G}^{\infty}))$ is embedded into $\mathrm{Out}(\overline{G}^{\infty}) \cong \mathbb{Z}_2$, we obtain $|\overline{G}| = 60n$ or $|\overline{G}| = 120n$. If $n \mid (p - 1)$, then $|\overline{G}| = (p^d - 1)/2$ implies that $(p^d - 1)/(p - 1)$ divides 240. For $d = 3, 4$ there is no prime with this property. If $n \mid (p^2 - 1)$, then $d = 4$ and $(p^2 + 1) \mid 240$. Again a direct check shows that there is no prime $p \geqslant 7$ satisfies this property.

Case (D2). p divides $|\overline{G}|$.

Since $p \geqslant 7$, p is coprime to $|\mathrm{Aut}(\overline{G}^{\infty})|$ and, therefore each p-subgroup of $\overline{G}$ centralizes $\overline{G}^{\infty}$.

As before $k(p^f + 1) = p^d - 1$. Our first goal is to show that $p^d - 1$ has a Zsigmondy prime divisor. To do that it is enough to exclude the case of $d = 2$. Assume that this is the case. Let $g \in \overline{G}$ be an element of order p. Since $\mathbf{C}_N(g)$ is a non-trivial proper subgroup of N and $|N| = p^2$, we obtain $|\mathbf{C}_N(g)| = p$. Since $\overline{G}^{\infty}$ centralizes g, the subgroup $\mathbf{C}_N(g)$ should be $\overline{G}^{\infty}$-invariant. But this is impossible, because $\overline{G}^{\infty} \cong SL(2, 5)$ has no non-trivial one-dimensional representation. Thus $d \geqslant 3$ and $p^d - 1$ has a Zsigmondy prime divisor which we denote as z. If $z \geqslant 7$, then z is coprime to $|\mathrm{Aut}(SL(2, 5))|$ and Proposition 2.4 yields a contradiction. If $z < 7$, then it follows from $z \geqslant d + 1 \geqslant 4$ that $z = 5$. Pick an arbitrary $g \in \overline{G}$ of order p. As it was shown before g centralizes $\overline{G}^{\infty}$. The subgroup $\mathbf{C}_N(g)$ is a non-trivial proper subgroup of N of order p^s, say. So $1 \leqslant s < d$. Since g centralizes $\overline{G}^{\infty}$, the subgroup $\mathbf{C}_N(g)$ is $\overline{G}^{\infty}$-invariant. The group $\overline{G}^{\infty}$ acts semiregularly on N. Therefore $120 = |\overline{G}^{\infty}|$ divides $p^s - 1$. Thus 5 is not a Zsigmondy prime divisor of $p^d - 1$, a contradiction. □

3. An example

Let p be a prime, $p > 3$ and L a 5-dimensional Lie algebra over $\mathbb{Z}_p$ defined by the following relations

$$[b_1, b_2] = b_3, \qquad [b_1, b_3] = b_4, \qquad [b_2, b_3] = b_5, \qquad \forall 1 \leqslant i \leqslant 5 \quad [b_i, b_5] = [b_i, b_4] = 0. \tag{4}$$

The commutator $[x_1, \ldots, x_n]$ is left-normalized, that is $[x_1, \ldots, x_n] := [[\ldots[x_1, x_2], \ldots], x_n]$.

It follows from (4) that

$$[L, L] = \langle b_3, b_4, b_5 \rangle, \qquad [L, L, L] = \langle b_4, b_5 \rangle, \qquad [L, L, L, L] = 0.$$

The structure of a p-group on L may be defined by Baker–Campbell–Hausdorff formula (see, for example, [12])

$$e^x e^y = e^v, \quad \text{where } v := x + y - \frac{1}{2}[y,x] + \frac{1}{12}[y,x,x] - \frac{1}{12}[y,x,y], \tag{5}$$

$$\left[e^y, e^x\right] = e^w, \quad \text{where } w := [y,x] + \frac{1}{2}[y,x,x] + \frac{1}{2}[y,x,y]. \tag{6}$$

We let U denote that group, and we use the formal exponent e^u, $u \in L$ in order to distinguish between the group and Lie algebra structures on L.

It is clear that any automorphism F of L gives rise to an automorphism of U

$$e^x \mapsto e^{F(x)}. \tag{7}$$

In the sequel we write each automorphism of L as a 5×5 matrix. We also define an action of $\mathsf{Aut}(L)$ on U by $(e^x)^F := e^{F^{-1}(x)}$.

An inner automorphism $e^x \mapsto e^{-a} e^x e^a$ of U has the following form

$$e^x \mapsto e^{x+[x,a]+\frac{1}{2}[x,a,a]}. \tag{8}$$

We let E_a denote the matrix of the linear mapping $x \mapsto x + [x,a] + \frac{1}{2}[x,a,a]$. Writing $a = \sum_{i=1}^{5} a_i e_i$, we obtain that

$$E_a = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ a_2 & -a_1 & 1 & 0 & 0 \\ a_3 - \frac{a_1 a_2}{2} & \frac{a_1^2}{2} & -a_1 & 1 & 0 \\ -\frac{a_2^2}{2} & a_3 + \frac{a_1 a_2}{2} & -a_2 & 0 & 1 \end{pmatrix}.$$

The following statement is straightforward.

Proposition 3.1. *The group U is of nilpotency class three and*

(a) $\mathbf{Z}(U) = e^{\langle b_4, b_5 \rangle}$;
(b) $U' = e^{\langle b_3, b_4, b_5 \rangle}$ *is elementary abelian*;
(c) $g^U = g\mathbf{Z}(U)$ *for each* $g \in U' \setminus \mathbf{Z}(U)$;
(d) $|g^U| = p^2$ *for each* $g \in U \setminus U'$.

Let us assume now that $p = 5$. Consider the following automorphisms of L:

$$T := \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 \end{pmatrix}, \qquad R := \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 \\ -1 & 1 & 0 & 1 & -1 \end{pmatrix},$$

$$S := RT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & 0 & 1 & 0 \\ -2 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Let Γ be the subgroup of $\mathsf{Aut}(L)$ generated by T and R. A direct check shows that the matrices T and R satisfy the following equalities

$$T^4 = R^3 = \big[T^2, R\big] = (TR)^5 = I_5.$$

These are defining relations of $SL(2,5)$. Therefore Γ is a homomorphic image of $SL(2,5)$. The restriction on the left-upper 2×2 submatrix is a homomorphism from Γ into $GL_2(5)$. Since the matrices $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$ generate $SL_2(5)$, this homomorphism is an isomorphism and we obtain $\Gamma = \langle T, R\rangle \cong SL_2(5)$. Each matrix from Γ acts on U according to (7). In what follows we identify matrices from Γ with automorphisms of U.

Proposition 3.2. *Let $\mathcal{C} = \{g^U \mid g \in U \setminus U'\}$. Then Γ acts transitively on $\mathcal{C}$.*

Proof. According to Proposition 3.1 each $C \in \mathcal{C}$ contains p^2 elements. Hence $|\mathcal{C}| = p(p^2-1)$ and our statement is equivalent to saying that Γ acts on $\mathcal{C}$ regularly. Let $g \mapsto \overline{g} := gU'$, $g \in U$ be the natural epimorphism. The action of Γ on $\overline{U} \cong \mathbb{Z}_p^2$ is equivalent to the action of $SL(2,p)$ on its natural module. Since $\overline{\mathcal{C}}$ is a set of non-identity elements of $\overline{U}$, the group Γ acts transitively on $\overline{\mathcal{C}}$. Since $|\overline{\mathcal{C}}| = p^2 - 1$, the stabilizer of $C \in \mathcal{C}$ in Γ is contained in a Sylow p-subgroup of Γ. Since all Sylow p-subgroups are conjugate, we may choose C such that its stabilizer is contained in $\langle S\rangle$. Assuming, towards a contradiction, that the stabilizer is non-trivial, we obtain that S fixes C setwise. Pick an arbitrary $g \in C$. Then $g = e^v$ for some $v \in L \setminus [L,L]$. It follows from $C^S = C$ that $g^{S^{-1}} = e^{S(v)} \in C$ implying $e^{S(v)} = e^{E_a(v)}$ for some $a \in L$. Therefore $S(v) = E_a(v)$ implying $v \in \ker(S - E_a)$. But it follows from the formulae for S and E_a that $\ker(S - E_a) \leqslant \langle b_3, b_4, b_5\rangle = [L,L]$, a contradiction. □

Let $G = \Gamma \ltimes U$ where the elements of Γ act on U according to (7). The elements of G will be written as ah, $h \in U$, $a \in \Gamma$ and $(ah)(a'h') = aa'h^{a'}h'$.

Theorem 3.3. *$(G, \mathbf{Z}(U))$ is a Camina pair.*

Proof. Since Γ acts on $\mathbf{Z}(U)$ p'-semiregularly, the action of G on $\mathbf{Z}(U)$ (by conjugation) is p'-semiregular too. Therefore $g^{\mathbf{Z}(U)} = g\mathbf{Z}(U)$ for each non-p-element $g \in G$.

Let now $g \in G \setminus \mathbf{Z}(U)$ be a p-element. If $g \in U' \setminus \mathbf{Z}(U)$, then by Proposition 3.1 $g^U = g\mathbf{Z}(U)$ implying $g^G \supseteq g\mathbf{Z}(U)$. If $g \in U \setminus U'$, then Proposition 3.2 implies that $g^G = U \setminus U'$.

Let now g be a p-element outside of U. We may assume that $g \in \langle S\rangle U \setminus U$ because $\langle S\rangle U$ is a Sylow p-subgroup of G. Thus $g = S^i h$ for some $i \in [1, p-1]$ and $h \in U$. Without loss of generality we may assume that $i = -1$. It is more convenient to write g as $g = S^{-1}h^{-1}$.

Pick an arbitrary $z \in \mathbf{Z}(U)$. We are looking for $x \in U$ such that $[g,x] = z$, or, equivalently, $x^{-g}x = z$. It is more convenient to change x to x^{-1} and rewrite the equation as

$$x^g x^{-1} = z \quad\Leftrightarrow\quad x^g = zx \quad\Leftrightarrow\quad x^{S^{-1}h^{-1}} = zx \quad\Leftrightarrow\quad x^{S^{-1}} = z^h x^h = zx^h.$$

Writing $x = e^v$, $z = e^w$, $h = e^a$ we obtain

$$e^{S(v)} = x^{S^{-1}} = zx^h = e^w e^{E_a(v)} = e^{E_a(v)+w} \quad\Leftrightarrow\quad S(v) = E_a(v) + w \quad\Leftrightarrow\quad w \in \mathrm{Im}(S - E_a).$$

Now a direct check shows that $\langle b_4, b_5\rangle \leqslant \mathrm{Im}(S - E_a)$ holds for each $a \in L$. □

Since the group U is defined for $p > 3$, one can construct a semi-direct product $\Gamma \ltimes U$ with $\Gamma \leqslant \mathrm{Aut}(L)$, $\Gamma \cong SL(2,p)$ for any prime $p > 3$. Unfortunately, the group $\Gamma \ltimes U$ does not produce a Camina pair if $p > 5$. The reason is that no subgroup $\Gamma \leqslant \mathrm{Aut}(L)$ isomorphic to $SL(2,p)$ has the property $\langle b_4, b_5\rangle \leqslant \mathrm{Im}(S - E_a)$ needed in the proof of Theorem 3.3 (here S is a generator of a Sylow p-subgroup of Γ).

Acknowledgments

The authors are very grateful to M. Herzog for valuable comments. We are also thankful to S.M. Gagola and C. Scoppola for pointing out errors in the preliminary manuscript. We are indebted to the anonymous referee for valuable remarks.

References

[1] Z. Arad, H. Blau, On table algebras and application to finite group theory, J. Algebra 138 (1991) 137–185.
[2] A. Arad, E. Fisman, An analogy between products of two conjugacy classes and products of two irreducible characters in finite groups, Proc. Edinb. Math. Soc. 30 (1987) 7–22.
[3] A.R. Camina, Some conditions which almost characterize Frobenius groups, Israel J. Math. 47 (1978) 153–160.
[4] P. Fleischmann, W. Lempken, P.H. Tiep, Finite p'-semiregular groups, J. Algebra 188 (1997) 547–579.
[5] S.M. Gagola, Characters vanishing on all but two conjugacy classes, Pacific J. Math. 109 (1983) 363–385.
[6] D. Chillag, A. Mann, C. Scoppola, Generalized Frobenius groups II, Israel J. Math. 62 (1988) 269–282.
[7] L.E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Dover Publications, New York, 1958.
[8] E.B. Kuisch, R.W. van der Waall, Homogeneous character induction, J. Algebra 149 (1992) 454–471.
[9] M. Liebeck, The affine permutation groups of rank three, Proc. London Math. Soc. 54 (3) (1987) 477–516.
[10] A. Mann, Products of classes and characters in finite groups, preprint.
[11] D.S. Passman, Permutation Groups, Benjamin, New York, 1968.
[12] M.F. Newman, E.A. O'Brien, M.R. Vaughan-Lee, Groups and nilpotent Lie rings whose order is the sixth power of a prime, J. Algebra 278 (2003) 383–401.
[13] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. 3 (1) (1892) 265–284.